

iPBX

USER GUIDE

Model: iPBX
Version 0.0.7
User Manual

Index

INDEX.....	2
ABOUT THIS MANUAL	4
COPYRIGHT DECLARATIONS	4
TRADEMARKS.....	4
SAFETY INSTRUCTIONS	4
WARRANTY	5
<i>Note</i>	5
INTRODUCTION IPBX.....	6
I-PBX SPECIFICATION.....	7
IP PHONE KEY SPECIFICATION:	7
IP SPECIFICATION	7
CONFIGURATION MANAGEMENT	8
HARDWARE SPECIFICATION	8
Front Panel Led indicators	8
Rear Panel.....	9
PACKET CONTENT	9
INSTALLATION:.....	10
Connecting to a PC / IPPHONE:.....	10
Connecting to an External Ethernet Hub or Switch:	10
QUICK START.....	11
How to set your network environment?	11
How to configure IPBX?	11
WIZARD SETUP.....	11
Setup 1. WAN type	12
Setup 2. NAT setup	13
Setup 3. IP PBX Setup.....	14
NETWORK SETUP.....	15
WAN SETTINGS.....	15
<i>Static IP</i>	16
<i>DHCP</i>	16
<i>PPPoE</i>	17
<i>Host Name</i>	17
<i>WAN Port MAC</i>	17

<i>MTU and MRU</i>	18
<i>DNS Server</i>	19
<i>Ping From WAN</i>	19
<i>LAN Setting</i>	19
<i>DNS Proxy</i>	20
LAN SETTING.....	20
DHCP SERVER SETTING	21
STATIC ROUTER	22
NAT SETTING.....	22
<i>NAT Setting</i>	23
<i>Virtual Server Setting</i>	24
<i>Port Trigger</i>	25
PACKET FILTER.....	26
URL FILTER	27
SECURITY	27
UPNP	28
DDNS.....	28
SNMP	29
IPBX.....	31
SIP BASIC SETTINGS	31
USER EXTENSIONS SETTING	33
Extensions List.....	33
Edit Extension Page.....	33
INCOMING RULES	35
RECORD VOICE MENU	35
CALL PARKING	36
ATTENDANT EXTENSION	37
DIALING RULES	38
GENERAL SETTING	39
MANAGEMENT	41
ADMIN ACCOUNT	41
DATE & TIME.....	42
PING TEST	43
SAVE & RESTORE	43
FACTORY DEFAULT.....	43
FIRMWARE UPDATE.....	44
IPBX SCENARIO APPLICATION SAMPLE	45

PREFACES

About This Manual

This manual is designed to assist users in using iPBX. Information in this document has been carefully checked for accuracy; however, no guarantee is given as to the correctness of the contents. The information contained in this document is subject to change without notice.

Copyright Declarations

Copyright 2006 Telephony Corporation. All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

Products and Corporate names appearing in this manual may or not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without to infringe.

Safety Instructions

The most careful attention has been devoted to quality standards in the manufacture of the iPBX. Safety is a major factor in the design of every set. But, safety is your responsibility too.

Use only the required power voltage. Power Input: AC 100-240V, 50-60Hz

To reduce the risk of electric shock, do not disassemble this product. Opening or removing covers may expose the iPBX to hazardous voltages. Incorrect reassembly can cause electric shock when this product is subsequently used.

Never push objects of any kind into the equipment through housing slots since they may touch hazardous voltage points or short out parts those could result in a risk of electric shock. Never spill liquid of any kind on the product. If liquid is spilled, please refer to the proper service personnel.

Use only Unshielded Twisted Pair (UTP) Category 5 Ethernet cable to RJ-45 port of the iPBX.

Warranty

We warrant to the original end user (purchaser) that the iPBX PBX will be free from any defects in workmanship or materials for a period of one (1) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to re-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors.

Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. We shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact us for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by us to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Introduction iPBX

iPBX has successfully combined the rich features of IP-PBX with built-in SIP Proxy Server to provide high effective, efficient and economical Voice over IP solution for SOHO to small enterprises users.

Users are able to integrate various VoIP networks into one total solution, as iPBX works with SIP compatible telephony devices (IP Phone, Soft Phone, Gateway, Wi-Fi Gateway, GSM Gateway), and allow more flexibility on business telephone system layout.

The following sections will provide users a comprehensive but straightforward user guides to iPBX. The sections covered the basic web configuration, setup procedures, and PBX setup and so on.

I-PBX Specification

IP Phone Key Specification:

1. Voice Codec: G.711 (A-law / μ -law), ilbc, gsm, G723, G726, G729
2. Call Waiting Music on hold / Resume
3. Call Transfer
4. Call Forward: Direct (IP-Phone , Web Control)
5. Call Forward: On Busy Forward (IP-Phone , Web Control)
6. Call Forward: No answer Forward (IP-Phone , Web Control)
7. Call Group (from Incoming call)
8. Call Pickup (IP-Phone dial pickup , same group)
9. Auto-attendant (incoming call)
10. 3-Way Conference
11. Outgoing dial authentication
12. Caller ID
13. Call Park
14. Dial Voice mail control (Message to Email / Voice to Email)

IP Specification

1. SIP (RFC 3261) , SDP (RFC 2327), Symmetric RTP,
2. Build-in SIP Server (for 20 Users Registrations) ,Service providers (for 6 Services providers).
3. Voice Codec: G.711 (A-law / μ -law), G.726 (16, 24, 32, 40 Kbps) , GSM ,ILBC, G723, G729 .
4. DTMF Support: DTMF Relay, info, In-band.
5. LAN : NAT, DHCP Server
6. WAN: PPPoE client, DHCP client, Fix IP Address, DDNS client
7. Network Address Translation: Providing build-in NAT router function.
8. Static Routing
9. Virtual DMZ
10. Port Mapping

Configuration Management

1. Web-based Graphical User Interface
2. Remote management over the IP Network.
3. Web firmware upgrade.
4. Backup and Restore Configuration file.

Hardware Specification

1. WAN: 1 x RJ-45 connectors used on 10BaseT and 100BaseTX networks.
2. LAN: 1 x RJ-45 connectors used on 10BaseT and 100BaseTX networks.
3. LED: 1 LED for Power Status / 1 LED for WAN Status / 1 LED for LAN Status.
4. AC power : AC100V-240V, DC12V/1.5A,50/60 Hz
5. Temperature: 0°C ~ 40°C (Operation)
6. Humidity: up to 90% non-condensing
7. Emission: FCC Part 15 Class B, CE Mark
8. Dimension : 170 x 100 x 35 mm
9. Weight: 165g

Front Panel Led indicators



Indicator	Status	Description
Power	ON	PBX Power ON
	OFF	PBX Power OFF
	ON	PBX network connection established.
WAN Port	Flashing	Data traffic on cable network
	OFF	Waiting for network connection
	ON	LAN is connected successfully
LAN Port	Flashing	Data is transmitting
	OFF	Ethernet not connected to PC

Rear Panel



Item	Status	Description
1	AC power (DC in 12V)	A power supply cable is inserted
2	Reset (Reset Button)	Push this button until 3 seconds, and iPBX will be set to factory default configuration.
3	WAN (Wide Area network)	Connect to the network with an Ethernet cable. This port allows your IPBX to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.
4	LAN (Local Area network)	Connect to PC with Ethernet cable. 1 port allows your PC or Switch/Hub to be connected to the IPBX through a networking cable with RJ-45 connectors used on 10BaseT and 100BaseTX networks.

Packet Content



(AC Power Adapter)



(iPBX Main)



(RJ-45 Cable)



(CD-ROM)

The IPBX packet contents:

IPBX(IPBX / WIPBX Series)	X1
RJ-45 Cable	X1
AC Power Adapter (12V)	X1
CD-Rom(User manual)	X1

Installation:

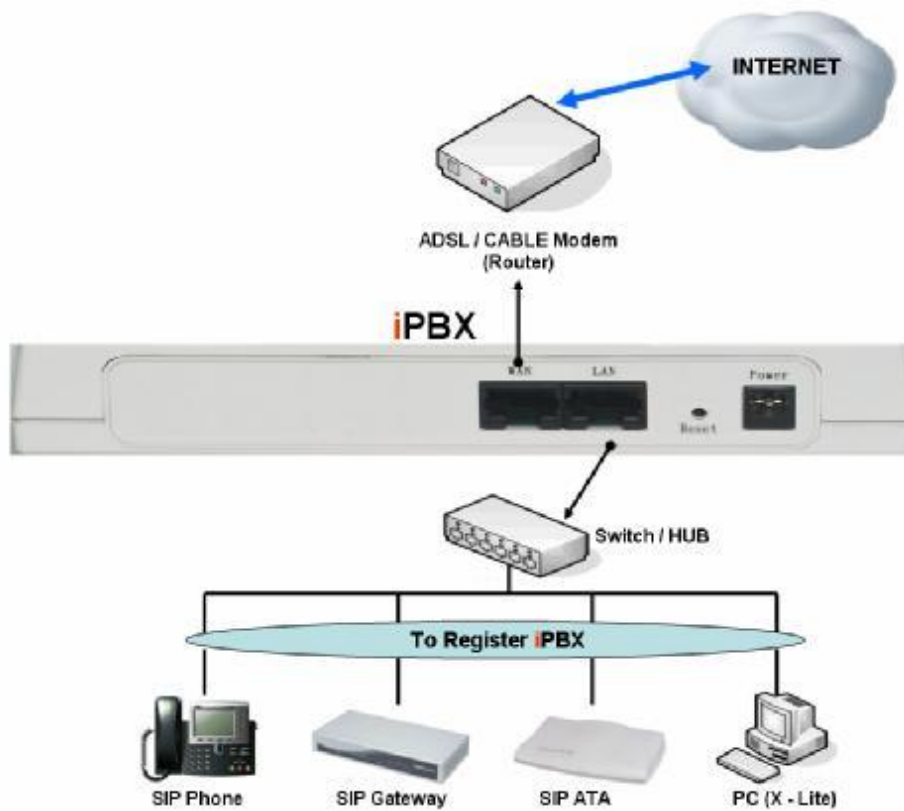
First, connect the 12V DC IN to the power outlet with power adaptor.

Connecting to a PC / IPPHONE:

1. Connect the Ethernet cable (with RJ-45 connector) to LAN port.
2. Connect the other end of the Ethernet cable to your PC's installed network interface card (NIC).

Connecting to an External Ethernet Hub or Switch:

1. Connect the Ethernet cable (with RJ-45 connector) to WAN port.
2. Connect the other end of the Ethernet cable to DSL/Cable modem or the external Ethernet hub or switch.



Quick Start

How to set your network environment?

iPBX default network environment:

For WAN:

IP: 192.168.1.1

Subnet mask: 255.255.0.0

Default Gateway: 192.168.1.254

For LAN:

IP: 222.222.222.1

Subnet mask: 255.255.0.0

Default Gateway: 222.222.222.254

How to configure IPBX?

1. Configure your PC or NB to the same subnet with **iPBX**.
2. Use web browser (IE / Firefox) link to url: <http://192.168.1.1:8888> (If you connect to LAN port, link to url: <http://222.222.222.1>)
3. Login user name: **admin**
4. Login password: **admin**
5. Use this web configuration interface to configure all system functionality; firstly you should change the WAN network environment to yours.

Wizard Setup

Wizard for Quick Setup of the **IPBX**, after finishing the authentication, the Main menu will display 3 parts of configuration, please click "Wizard Setup" to enter quick start

Setup 1. WAN type

The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click “**WAN Type**” from within the Wizard **Setup**, the following setup page will be show.

Three methods are available for Internet Access:

Step 1.WAN Type

Please specify the WAN connection type required. Please select one of these three types: DHCP Client for Cable modem, Fixed-IP , or PPPoE for ADSL modem.

- **Static - IP**
Internet Service Providers may assign a static IP address for your VoIP Router. Select this option and enter the assigned IP address, subnet mask, gateway IP and DNS IP addresses for your Barricade.
- **DHCP - Cable Modem**
This function will be automatically configured when plugged into the cable modem. If there is a Domain Name Server (DNS) that you would input to use.
- **PPPoE - ADSL**
If you connect to the Internet using an ADSL Modem, please enter the username and password which provided from ISP.

- I. **Fixed – IP User:** If you are a leased line user with a fixed IP address, fill out the following items with the information provided by your ISP.

• **Static - IP**

WAN IP Address	<input type="text" value="10.10.10.230"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Getway	<input type="text" value="10.10.10.1"/>

WAN IP Address : check with your ISP provider

Subnet Mask : check with your ISP provider

Default Gateway : check with your ISP provider

- II. **DHCP – Cable Modem User** : Get WAN IP Address automatically

DHCP Client Enabled !

IP Address: If you are connected to the Internet through a Cable modem line then a dynamic IP address will be assigned.

- III. **ADSL Dial-Up User (PPPoE Enable):** Some ISP's provide DSL-based service and use PPPoE to establish communication link with end-users. If you are connected to the Internet through a DSL line,

check with your ISP to see if they use PPPoE. If they do, you need to select this item.

- **PPPoE - ADSL**

Enter the User Name and Password required by your ISP.

PPPoE Username : (MAX. 40 characters)
PPPoE Password : (MAX. 40 characters)
confirmation password : (MAX. 40 characters)

Previous

Next

PPPoE User Name: Enter User Name provided by your ISP

PPPoE Password: Enter Password provided by your ISP

Confirmation Password: Enter Password to confirm again

Setup 2. NAT setup

NAT (Network Address Translation) is a method of connecting multiple computer's to the Internet using one IP address.

Step 2.NAT Setting

You can use NAT to allow PCs from LAN subnet for accessing Internet

- **LAN IP Setting**

LAN IP Address
Subnet Mask
DHCP Server ☒ Enable
Assigned DHCP IP Address Start IP:
End IP :
DHCP IP Lease Time seconds (60..864000)

LAN IP Address: Private IP address for connecting to a local private network (Default: 222.222.222.1).

Subnet Mask: Subnet mask for the local private network (Default: 255.255.255.0).

DHCP Server: Enable to open LAN port DHCP server.

Assigned DHCP IP Address: DHCP server range from start IP to end IP.

DHCP IP Lease Time: Client to ask DHCP server refresh time, range from 60 to 86400 seconds

Setup 3. IP PBX Setup

The iPBX allows multiple ITSP providers / User Extensions registration by simply fill-in the required information in the provided table. . .

Step 3.IPBX Wizard Setup

Add Service Provider **Service Provider Max is 10**

Caller Id	UserName	Password	Host	Port	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>
0078985232	0078985232	0078985232	www.server02.com	5060	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
0988321456	0988321456	0988321456	www.server01.com	5060	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Add User Extensions **Extension Max is 30**

User Extension	Password	Caller Id	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>
202	202	202	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
203	203	203	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Service Provider:

Caller ID: service provider name

Username: Input Provider name

Password: Input Provider password

Host: Input Providers server address

Port: Providers server port

User Extensions

User Extension: Input Extension number

Password: Input Extension password

Caller id: Input Extension caller id

After completing the wizard setup, click “Finish” button, The iPBX will save configuration and reboot iPBX automatically, after 30 – 40 seconds, you can re-load setting page again.

Network Setup

WAN Settings

WAN (Wide Area Network) is a network connection connecting one or more LANs together over some distance. For example, the means of connecting two office buildings separated by several kilometers would be referred to as a WAN connection. The size of a WAN and the number of distinct LANs connected to a WAN is not limited by any definition. Therefore, the Internet may be called a WAN.

WAN Settings are settings that are used to connect to your ISP (Internet Service Provider). The WAN settings are provided to you by your ISP and often times referred to as "public settings". Please select the appropriate option for your specific ISP.

For most users, Internet access is the primary application. IP-PBX supports the WAN interface for internet access and remote access. The following sections will explain more details of WAN Port Internet access and broadband access setup. When you click "WAN Setting", the following setup page will be shown. Three methods are available for Internet Access.

Network Settings

• WAN Setting

NAT / Bridge Mode	<input type="text" value="NAT"/>
WAN Port IP Assignment	<input checked="" type="radio"/> Static IP <input type="radio"/> DHCP <input type="radio"/> PPPoE
Host Name	<input type="text" value="SIP"/> . <input type="text" value="ATA"/>
WAN Port MAC	<input checked="" type="radio"/> Original MAC (00:0C:29:FD:1E:4C) <input type="radio"/> Manual Setting <input type="text" value="00:00:27:88:81:18"/>
IP Address	<input type="text" value="192.168.1.2"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
MTU	<input type="text" value="1500"/> bytes
MRU	<input type="text" value="1500"/> bytes
Primary DNS Server	<input type="text" value="168.95.1.1"/>
Secondary DNS Server	<input type="text" value="168.95.192.1"/>
Ping from WAN	<input checked="" type="checkbox"/> Allowed

• LAN Setting

LAN IP Address	<input type="text" value="222.222.222.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DNS Proxy	<input checked="" type="checkbox"/> Enable

Submit

Reset

Static IP

If you are a leased line user with a fixed IP address, enter in the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. *Example: 168.95.1.2*

• WAN Setting

WAN Port IP Assignment	<input checked="" type="radio"/> Static IP	<input type="radio"/> DHCP	<input type="radio"/> PPPoE
Host Name	<input type="text" value="SA200"/> . <input type="text" value="ATA.com"/>		
WAN Port MAC	<input checked="" type="radio"/> Original MAC (00:35:56:70:62:D0)	<input type="radio"/> Manual Setting <input type="text" value="01:20:27:88:81:18"/>	
IP Address	<input type="text" value="168.95.1.2"/>		
Subnet Mask	<input type="text" value="255.255.255.0"/> ▼		
Default Gateway	<input type="text" value="168.95.1.254"/>		

IP Address: Check with your ISP provider.

Subnet Mask: Check with your ISP provider.

Default Gateway: Check with your ISP provider.

DHCP

Dynamic Host Configuration Protocol (DHCP), Dynamic IP (Get WAN IP Address automatically). If you are connected to the Internet through a Cable modem line, then a dynamic IP will be assigned.

Note: WAN port gets the IP Address, Subnet Mask and default gateway IP address automatically, if DHCP client is successful.

• WAN Setting

WAN Port IP Assignment	<input type="radio"/> Static IP	<input checked="" type="radio"/> DHCP	<input type="radio"/> PPPoE
Host Name	<input type="text" value="SA200"/> . <input type="text" value="ATA.com"/>		
WAN Port MAC	<input checked="" type="radio"/> Original MAC (00:35:56:70:62:D0)	<input type="radio"/> Manual Setting <input type="text" value="01:20:27:88:81:18"/>	
MTU	<input type="text" value="1500"/>	bytes	
MRU	<input type="text" value="1500"/>	bytes	
Set DNS server	<input type="radio"/> Manually	<input checked="" type="radio"/> Automatically	
Ping from WAN	<input checked="" type="checkbox"/> Allowed		

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE). Some ISPs provide DSL-based services and use PPPoE to establish communication link with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to make sure the following items, PPPoE User name: Enter username provided by your ISP. PPPoE Password: Enter password provided by your ISP.

• WAN Setting

WAN Port IP Assignment	<input type="radio"/> Static IP	<input type="radio"/> DHCP	<input checked="" type="radio"/> PPPoE
Host Name	<input type="text" value="SA200"/> . <input type="text" value="ATA.com"/>		
WAN Port MAC	<input checked="" type="radio"/> Original MAC (00:35:56:70:62:D0)		
	<input type="radio"/> Manual Setting <input type="text" value="01:20:27:88:81:18"/>		
PPPoE Username	<input type="text" value="PPPOE USERNAM"/>		
PPPoE Password	<input type="password" value="....."/>		
MTU	<input type="text" value="1492"/>	bytes	
MRU	<input type="text" value="1492"/>	bytes	
Set DNS server	<input type="radio"/> Manually <input checked="" type="radio"/> Automatically		
Ping from WAN	<input checked="" type="checkbox"/> Allowed		

Host Name

The Host Name field is optional but may be required by some Internet Service Providers. The default host name is the model number of the device. It is a computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address. Assign the domain name or IP address of your host computer. When the host operating system is set up it is given a name. This name may reflect the prime use of the computer. For example, a host computer that converts host names to IP addresses using DNS may be called cvs.IP-PBX.com and a host computer that is a web server may be called www.IP-PBX.com. When we need to find the host name from an IP address we send a request to the host using its IP address. The host will respond with its host name.

Host Name	<input type="text" value="SA200"/>	.	<input type="text" value="ATA.com"/>
-----------	------------------------------------	---	--------------------------------------

WAN Port MAC

The MAC (Media Access Control) Address field is required by some Internet Service Providers (ISP). The default MAC address is set to the MAC address of the WAN interface in the device. It is only necessary to fill the field if required by your ISP.

The WAN port allows your voice gateway to be connected to an Internet Access Device, e.g. router, cable modem, ADSL modem, through a CAT.5 twisted pair Ethernet Cable. MAC addresses are uniquely set by the network adapter manufacturer and are sometimes called "physical addresses" for this reason. MAC assigns a unique number to each IP network adapter called the MAC address. The MAC address is commonly written as a sequence of 12 hexadecimal digits as follows: 00:0f:fd: 88:81:18 The first six hexadecimal digits of the address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number.

Some Internet service providers track the MAC address of a home router for security purposes. Many routers support a process called cloning that allows the MAC address to be simulated so that it matches one the service provider is expecting. This allows end-user to change their router (and their real MAC address) without having to notify the provider. For example, you could allow packets which have your name server's IP on them, but come from another MAC address (one way of spoofing packets).



MTU and MRU

MTU stands for Maximum Transmission Unit, the largest physical packet size, measured in bytes that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

MRU stands for Maximum Receiving Unit. The largest physical packet size, measured in bytes that a network can receive. Any messages larger than the MRU are divided into smaller packets before being received.

The key is to be deciding how big your bandwidth pipe is and select the best MTU for your configuration. For example, you have a 33.6 modem, you use a MTU and MRU of 576, and if you have a larger pipe you may want to try 1500.



Note:

- For Static IP, both MTU and MRU are set to 1500 bytes as default value.
- For DHCP, both MTU and MRU are set to 1500 bytes as default value.
- For PPPoE, both MTU and MRU are set to 1492 bytes as default value.

DNS Server

DNS stands for Domain Name System. Every Internet host must have a unique IP address; also they may have a user-friendly, easy to remember name such as www.ipbx.com. The DNS server converts the user-friendly name into its equivalent IP address. The original DNS specifications require that each domain name is served by at least 2 DNS servers for redundancy. When you run your DNS, web, and mail servers all on the same MACHINE - if this MACHINE goes down, it doesn't really matter that the backup DNS server still works.

The recommended practice is to configure the primary and secondary DNS servers on separate MACHines, on separate Internet connections, and in separate geographic locations.

Primary DNS Server	<input type="text" value="168.95.1.1"/>
Secondary DNS Server	<input type="text" value="168.95.1.2"/>

Primary DNS Server: Sets the IP address of the primary DNS server.

Secondary DNS Server: Sets the IP address of the secondary DNS server.

Ping From WAN

Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating. The default setting is allowed user can ping the host computer from remote site. If you disallow, the host computer doesn't response any user who issues Ping IP address command from any remote sites.

Ping from WAN	<input checked="" type="checkbox"/> Allowed
---------------	---

LAN Setting

These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 222.222.222.1 with a subnet mask of 255.255.255.0.

LAN is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

• LAN Setting

LAN IP Address	<input type="text" value="222.222.222.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/> ▼
DNS Proxy	<input checked="" type="checkbox"/> Enable

LAN IP Address: Assign the IP address of LAN server, default is 222.222.222.1

Subnet Mask: Select a subnet mask from the pull-down menu, default is 255.255.255.0.

DNS Proxy

A proxy server is a computer network service that allows clients to make indirect network connections to other network services. The default setting is Enable the DNS proxy server.

DNS Proxy	<input checked="" type="checkbox"/> Enable
-----------	--

LAN Setting

These are the IP settings of the LAN (Local Area Network) interface for the device. These settings may be referred to as "private settings". You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 222.222.222.1 with a subnet mask of 255.255.255.0.

LAN is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

• LAN Setting

LAN IP Address	<input type="text" value="222.222.222.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/> ▼
DNS Proxy	<input checked="" type="checkbox"/> Enable

LAN IP Address: Assign the IP address of LAN server, default is 222.222.222.1

Subnet Mask: Select a subnet mask from the pull-down menu, default is 255.255.255.0.

DHCP Server Setting

DHCP stands for Dynamic Host Control Protocol. The DHCP server gives out IP addresses when a device is starting up and request an IP address to be logged on to the network. The device must be set as a DHCP client to "Obtain the IP address automatically". By default, the DHCP Server is enabled in the unit. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP client computers connected to the unit will have their information displayed in the DHCP Client List table. The table will show the Type, Host Name, IP Address, MAC Address, Description, and Expired Time of the DHCP lease for each client computer. DHCP Server is a useful tool that automates the assignment of IP addresses to numbers of computers in your network. The server maintains a pool of IP addresses that you use to create scopes. (A DHCP scope is a collection of IP addresses and TCP/IP configuration parameters that are available for DHCP clients to lease.) Then, the server automatically allocates these IP addresses and related TCP/IP configuration settings to DHCP-enabled clients in the network. The DHCP Server leases the IP addresses to clients for a period that you specify when you create a scope. A lease becomes inactive when it expires. Through the DHCP Server, you can reserve specific IP addresses permanently for hardware devices that must have a static IP address (e.g., a DNS Server).

An advantage of using DHCP is that the service assigns addresses dynamically. The DHCP Server returns addresses that are no longer in use to the IP addresses pool so that the server can reallocate them to other machines in the network. If you disable this DHCP, you would have to manually configure IP for new computers, keep track of IP addresses so that you could reassign addresses that clients aren't using, and reconfigure computers that you move from one subnet to another. The DHCP Static MAP table lists all MAC and IP address which are active now.

Network Settings

• DHCP Server Settings

DHCP Server	<input checked="" type="checkbox"/> Enable
Assigned DHCP IP Address	Start IP: 192.168.0. <input type="text"/>
	End IP : 192.168.0. <input type="text"/>
DHCP IP Lease Time	<input type="text"/> seconds (60..864000)
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

• DHCP Static Map

MAC	IP	Description	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

• DHCP Client List

Type	Hostname	MAC	IP	Expire Time
------	----------	-----	----	-------------

When you enable the DHCP server, you are able to enter:

Assigned DHCP IP Address: Enter the starting IP address for the DHCP server's IP assignment and the ending IP address for the DHCP server's IP assignment.

DHCP IP Lease Time: Assign the length of time for the IP lease, default setting is 86400 seconds.

Static Router

Static routes are special routes that the network administrator manually enters into the router configuration for local network management. You could build an entire network based on static routes. The problem with doing this is that when a network failure occurs, the static route will not change without you performing the change. This could be fIP-PBXI if the failure occurs when the administrator is not available.

The route table allows the user to configure and define all the static routes supported by the router.

Network Settings

• Static Route

Enable	Type	Target	Netmask	Gateway	Action
<input type="checkbox"/>	Net		255.255.255.0		Insert Change

Enable: Enable/Disable the static route.

Type: Indicates the type of route as follows, Host for local connection and Net for network connection.

Target: Defines the base IP address (Network Number) that will be compared with the destination IP address (after an AND with NetMask) to see if this is the target route.

NetMask: The subnet mask that will be AND'd with the destination IP address and then compared with the Target to see if this is the target route.

Gateway: The IP address of the next hop router that will be used to route traffic for this route. If this route is local (defines the locally connected hosts and Type = Host) then this IP address MUST be the IP address of the router

Action: Insert a new Static Router entry or update a specified entry.

NAT Setting

NAT (Network Address Translation) serves **three** purposes:

1. Provides security by hiding internal IP addresses. Acts like firewall.
2. Enables a company to access internal IP addresses. Internal IP addresses that are only available within

the company will not conflict with public IP.

3. Allows a company to combine multiple ISDN connections into a single internet connection.

Network Settings

• NAT Setting

Network Address Translation	<input checked="" type="checkbox"/> Enable
IPSec Pass Through	<input checked="" type="checkbox"/> Enable
PPTP Pass Through	<input checked="" type="checkbox"/> Enable
L2TP Pass Through	<input checked="" type="checkbox"/> Enable
SIP ALG	<input type="checkbox"/> Enable
NetMeeting ALG	<input type="checkbox"/> Enable
DMZ	<input type="checkbox"/> Enable

Submit

Reset

• Virtual Server Mapping

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

• Port Trigger

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="button" value="Insert"/> <input type="button" value="Change"/>

NAT Setting

• NAT Setting

Network Address Translation	<input checked="" type="checkbox"/> Enable
IPSec Pass Through	<input checked="" type="checkbox"/> Enable
PPTP Pass Through	<input checked="" type="checkbox"/> Enable
L2TP Pass Through	<input checked="" type="checkbox"/> Enable
SIP ALG	<input checked="" type="checkbox"/> Enable
DMZ	<input checked="" type="checkbox"/> Enable

DMZ LAN IP

Submit

Reset

Network Address Translation: Enable/Disable NAT.

IPSec Pass Through: IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. Enable/Disable this framework verification.

PPTP Pass Through: PPTP (Point-to-Point Tunneling Protocol) is a protocol that allows corporations to

extend their own corporate network through private "tunnels" over the public Internet. Enable/Disable this protocol verification.

L2TP Pass Through: L2TP (The Layer 2 Tunnel Protocol) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. Enable/Disable this function.

SIP ALG: SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. Enable/Disable this protocol verification.

DMZ: In computer networks, a DMZ (Demilitarized Zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company dIP-PBX. Think of DMZ as the front yard of your house. It belongs to you and you may put some things there, but you would put anything valuable inside the house where it can be properly secured. Setting up a DMZ is very easy. If you have multiple computer s, you can choose to simply place one of the computers between the Internet connection and the firewall.

DMZ IP LAN: If you have a computer that cannot run Internet applications properly from behind the device, then you can allow the computer to have unrestricted Internet access. Enter the IP address of that computer as a DMZ host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

Virtual Server Setting

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network. You will only need to input the LAN IP address of the computer running the service and enable it.

A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP.

• Virtual Server Mapping

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
<input type="checkbox"/>	80	TCP ▼	222.222.222.17	80	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Enable: Enable/Disable the virtual server mapping, default setting is Disable.

WAN Port: The port number on the WAN side that will be used to access the virtual service. Enter the WAN

Port number, e.g. enter 80 to represent the Web (http server), or enter 25 to represent SMTP (email server).

Note: You can specify maximum 32 WAN Ports.

Protocol: The protocol used for the virtual service. Select a protocol type is TCP or UDP.

LAN IP: The server computer in the LAN network that will be providing the virtual services. Enter the IP address of LAN.

LAN Port: The port number of the service used by the Private IP computer. Enter the LAN port number.

Action: Insert a new WAN port or update a specified WAN port.

Port Trigger

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP (Transmission Control Protocol) or UDP (User DIP-PBXgram Protocol), then enter the public ports associated with the trigger port to open them for inbound traffic.

• **Port Trigger**

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
<input type="checkbox"/>	40	TCP	40	TCP	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Enable: Enable/Disable the port trigger, default setting is Disable.

Trigger Port: This is the port used to trigger the application. It can be either a single port or a range of ports.

Trigger Type: This is the protocol used to trigger the special application.

Public Port: This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Public Type: This is the protocol used for the special application.

Action: Insert a new Port Trigger or update a specified Port Trigger.

Packet filter

Controlling access to a network by analyzing the incoming packets and letting them pass or halting them based on the IP addresses of the source. (This function can be useful for residential screening as well – for parental screening or other)

Network Settings

• Packet Filter

WAN ☒ Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	TCP	Always	All	00:00 ~ 00:00	<input type="button" value="Insert"/> <input type="button" value="Change"/>

LAN ☒ Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	TCP	Always	All	00:00 ~ 00:00	<input type="button" value="Insert"/> <input type="button" value="Change"/>

MAC ☒ Enable

Enable	MAC Address	Block	Day	Time	Action
<input type="checkbox"/>	<input type="text"/>	Always	All	00:00 ~ 00:00	<input type="button" value="Insert"/> <input type="button" value="Change"/>

WAN

WAN Enable/Disable: The WAN IP port packet filter function, control a network IP port, default setting is *Enable*.

Enable: Enable/Disable the Internet to WAN IP source port rules, default setting is *Disable*.

Source IP: This is the filter WAN IP address. *Example: 209.131.36.158*

Dest. Port: This is the port used for source IP service.

Protocol: This Protocol Used for the source IP service. Select either TCP or UDP.

Block: Wan IP Port Block time setting. Select *Always* or *By Schedule*.

Day: Block Day setting, select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.

Time: Block Time setting, select time range is 00:00 to 23:59.

LAN

LAN Enable/Disable: Internet to LAN filter function, default setting is *Enable*. A prohibitive rule set should only allow the necessary Internet/DMZ services to LAN (Local Area Network) clients.

Enable: Enable/Disable the WAN IP source port rules, default setting is *Disable*.

Source IP: This is the filter source IP address to LAN.

Dest. Port: This is the port used for source IP.

Protocol: This Protocol Used for the WAN Filter service. Select either TCP or UDP.

Day: Block Day setting, select All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.

Time: Block Time setting, select time range is 00:00 to 23:59

MAC

MAC Enable/Disable: Form internet MAC filter function, default setting is *Enable*.

Block: Wan IP Port Block time Setting. Select Always or *By Schedule*.

Day: Block Day setting, select a All / Mon-Sat./ Mon-Fri./Mon./ Tues./ Wed./Thu./Fri./Sat./Sun.

Time: Block Time setting, select time range is 00:00 to 23:59

URL Filter

URL filter allows you to block sites based on a black list and white list. Sites matching the black list but not matching the white list will be automatically blocked and closed.

Network Settings

• URL Filter

☒ Enable

Enable	Client IP	URL Filter String	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Enable: Enable/Disable the URL filter function, default setting is Disable.

Enable: Enable/Disable Block URL to the Client IP, default setting is Disable

Client IP: This is the Client IP is LAN address. *Example:* 222.222.222.100

URL Filter String: This is the filter URL. *Example:* "http://www.yahoo.com/"

Security

Intrusion Detection has powerful management and analysis tools that let your IT administrator see what's going on in your network. Such as who's surfing the Web, and gives you the tools to block access to inappropriate Web sites.

Malicious code (also called vandals) is a new breed of Internet threat that cannot be efficiently controlled by conventional antivirus software alone. In contrast to viruses that require a user to execute a program in order to cause damage, vandals are auto-executable applications

Network Settings

• Security Setting

Intrusion Detection ☒ Enable
Drop Malicious Packet ☒ Enable

Submit

Reset

Intrusion Detection: Enable / Disable , network / internet security protection.

Drop Malicious Packet: Enable / Disable , Detect and drop malicious application layer traffic.

UPNP

UPnP provides support for communication between control points and devices. The network media, the TCP/IP protocol suite and HTTP provide basic network connectivity and addressing needed. On top of these open, standard, Internet based protocols, UPnP defines a set of HTTP servers to handle discovery, description, control, events, and presentation.

Network Settings

• UPNP Setting

UPNP Internet Gate Device ☒ Enable

Submit

Reset

UPNP Internet Gate Device: Enable/Disable UPNP Service to working, default setting is *Disable*.

DDNS

The DDNS (Dynamic DNS) service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. Without DDNS, the users should use the WAN IP to reach internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported, you apply a DNS name (e.g., www.IP-PBX.com) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.IP-PBX.com regardless of the WAN IP.

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address, you can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname.

Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider.

DDNS is a method of keeping a domain name linked to a changing (dynamic) IP address. With most Cable and DSL connections, you are assigned a dynamic IP address and that address is used only for the duration of that specific connection. With the IP-PBX, you can setup your DDNS service and the IP-PBX will automatically update your DDNS server every time it receives a different IP address.

Network Settings

• DDNS Setting

DDNS	<input checked="" type="checkbox"/> Enable
DDNS Server Type	<input type="text" value="DynDns.org"/>
DDNS Username	<input type="text"/>
DDNS Password	<input type="password"/>
Confirmed Password	<input type="password"/>
Hostname to register	<input type="text"/>
DDNS Interval Registration	<input type="checkbox"/> Enable
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Enable: Enable/Disable the DDNS service, default setting is Disable.

DDNS Server Type: The IP-PBX support two types of DDNS, DynDns.org or No-IP.com

DDNS Username: The username which you register in DynDns.org or No-IP.com website.

DDNS Password: The password which you register in DynDns.org or No-IP.com website.

Confirmed Password: Confirm the password which you typing.

Hostname to register: The hostname which you register in DynDns.org or No-IP.com website

SNMP

The simple network management protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a dIP-PBXbase schema, and a set of dIP-PBX objects.

Network Settings

• SNMP Setting

SNMP	<input checked="" type="checkbox"/> Enable
SNMP Read Community	<input type="text" value="public"/> (default:public)
SNMP Write Community	<input type="text" value="private"/> (default:private)
SNMP Trap Host	<input type="text"/>
SNMP Trap Community	<input type="text" value="public"/> (default:public)

Enable: Enable/Disable the SNMP service, default setting is Disable. (Support SNMP version 1 or SNMP version 2c).

SNMP Read Community: SNMP Read Community string so that EPICenter can retrieve information.(default :public)

SNMP Write Community: Specifies the name of the SNMP write community to which the printer device that this actual destination represents belongs.(Default:private)

SNMP Trap Host: Defines an SNMP trap host to which AppCelera will send trap messages. (Default address is empty)

SNMP Trap Community: The SNMP trap community name. The community name functions as a password for sending trap notifications to the target SNMP manager.(Default : public).

iPBX

SIP basic Settings

SIP (Session Initiation Protocol) is a request-response protocol, dealing with requests from clients and responses from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

SIP Basic Setting

• SIP Configuration

UDP Port to bind to	<input type="text" value="5060"/>
Domain	<input type="text"/>
Allow guest calls	<input checked="" type="checkbox"/>
Allow Transfers	<input checked="" type="checkbox"/>
Overlap dialing support	<input checked="" type="checkbox"/>
Enable DNS SRV lookups (on outbound calls)	<input checked="" type="checkbox"/>
Min Registration/Subscription Time	<input type="text" value="900"/>
Max Registration/Subscription Time	<input type="text" value="3600"/>
Default Incoming/Outgoing Registration Time	<input type="text" value="900"/>
Min Roundtrip Time (T1 Time)	<input type="text" value="200"/>
Language	<input type="text" value="English"/>
Enable Relaxed DTMF	<input checked="" type="checkbox"/>
Server UserAgent	<input type="text" value="PBX"/>
DTMF Mode	<input type="text" value="rfc2833"/>

• SIP Codecs

Codec Priority 1	<input type="text" value="g726"/>
Codec Priority 2	<input type="text" value="alaw"/>
Codec Priority 3	<input type="text" value="ilbc"/>
Codec Priority 4	<input type="text" value="gsm"/>
Codec Priority 5	<input type="text" value="g723"/>
Codec Priority 6	<input type="text" value="g726"/>
Codec Priority 7	<input type="text" value="g729"/>

• Outbound SIP Registrations

Register TimeOut	<input type="text" value="20"/>
Register Attempts	<input type="text" value="65535"/>

• NAT Support

Extern IP	<input type="text"/>
Extern Refresh	<input type="text"/>
Local Network Address	<input type="text"/>
NAT mode	<input type="text" value="never"/>
Allow RTP Reinvite	<input type="text" value="nonat"/>

SIP Configuration

UDP Port to bind to: This is SIP Local Port 5060, if you have any specific reason for change this port.

Domain: IPBX Server's IP address.

Allow guest calls: Enable/Disable guest calls. Default is *Enable*. Default is all IP.

Overlap dialing support: Enable/Disable overlap dialing support . Default is *Enable*.

Allow Transfers: Enable Call Transfers.

Enable DNS SRV lookups (on outbound calls): Enable DNS SRV lookups on calls

Max Registration Time: Maximum duration of incoming registration/subscriptions we allow. Default 3600 seconds.

Min Registration Time: Minimum duration of registrations/subscriptions. Default 60 seconds

Default Incoming/Outgoing Registration Time: Default duration (in seconds) of incoming / outgoing

registration

Min RoundtripTime (T1 Time): Minimum roundtrip time for messages to monitored hosts, Defaults to *200 ms*

Language: Set default language for all users.

Enable Relaxed DTMF: Use relaxed DTMF detection . Default is *Disable*.

Server UserAgent: Enable you to change the trunk User agent string, Default is *PBX*.

DTMF Mode: Set default DTMF mode for sending DTMF. Default: *rfc2833*.

SIP Codecs

The Codec is used to compress the voice signal into data packets. Each Codec has different bandwidth requirement. There are 7 kinds of codec. To determine the priority, selects one codec algorithm from the pull-down menus individually.

Outbound SIP Registrations

Register TimeOut: Retry registration calls at every 'x' seconds (default 20)

Register Attempts: Number of registration attempts before we give up; 0 = continue forever

NAT Support

The *externip*, *externhost* and *localnet* settings are used if you use IPBX behind a NAT device to communicate with services on the outside.

Extern IP: Address that we're going to put in outbound SIP messages if we're behind a NAT

Extern Host: Alternatively you can specify an external host, and **iPBX** will perform DNS queries periodically.

Not recommended for production environments! Use *externip* instead

Extern Refresh: How often to refresh *externhost* if used. You may specify a local network in the field below

Local Network Address:

localnet=192.168.0.0/255.255.0.0; All RFC 1918 addresses are local networks

localnet=11.0.0.0/255.0.0.0 ; Also RFC1918

localnet=171.16.0.0/12 ; Another RFC1918 with CIDR notation

localnet=168.254.0.0/255.255.0.0; Zero conf local network

User Extensions Setting

Extensions List

User Extension	Password	Caller Id	Action		
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/>	<input type="button" value="Change"/>	
202	202	202	<input type="button" value="Edit"/>	<input type="button" value="Advance"/>	<input type="button" value="Delete"/>
203	203	203	<input type="button" value="Edit"/>	<input type="button" value="Advance"/>	<input type="button" value="Delete"/>

Edit: Click to edit an extension User extension / password / callerid

Advance: Click to edit an extension other setting

Delete: Click to delete an extension.

Edit Extension Page

User Extension Advance Setup

User Extension	102
Password	102
Caller Id	102

- **Call group / Pickup group select**

Call Group	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10
Pickup Group	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10
- **Call forward option**

Call Forward Always	<input type="text"/>
Call Forward on Busy	<input type="text"/>
Call Forward on No Answer	<input type="text"/>
	IF Time out <input type="text"/> Sec
- **Voice mail**

Voicemail	<input checked="" type="checkbox"/> Enable
Voicemail name	<input type="text"/>
Voicemail password	<input type="text"/>
E-mail address	<input type="text"/>
	<input type="checkbox"/> Send voice to mail
	<input type="checkbox"/> Delete voicemail after send

User Extension: Input Extension number

Password: Input Extension password

Caller id: Input Extension caller id

Call group / Pickup group select

Call Group: An Extension can set single/multiple call group(s) 1-10 id

Pickup Group: An Extension can set single/multiple Pickup group(s) 1-10 id

Call forward option

Call forward always: Input forward always number

Call forward on busy: Input forward on busy number

Call forward no answer: Input forward no answer number

If time out “XXX” sec: This is the maximum number allowed no answer time out used

Voice mail

Voice mail select: Enable / Disable voice mail function

Voice mail name: Input voice mail name

E-Mail address: Input E-mail address

Send voice to mail: Enable / Disable send voice to mail

Delete voice mail after send: Save / Delete voice mail after send

Incoming Rules

Defined **Service providers** based on date and time voice rule.

• Attendant Incoming Rules

Day Setting

Start Day

End Day

Time Setting

Start Time :

End Time :

Month Setting

Start Month

End Month

Date Setting

Start Date

End Date

Day setting : Defined Start day / end time .

Time setting : Defined Start time / End time .

Month setting : Defined Start Month / End Month .

Date setting : Defined Start Date / End Date .

Record Voice Menu

Allow you to record On / Off duty voice menu over a register ip-phone..

• Record Voice Menu

Record voice

Ex: *9

Play voice

Ex: *10

Default voice

Ex: *11

Password

Answer Extension

On - Off Duty

Pick up your register IP-Phone handset and press “function key + password “ to enter into voice menu guide.

- Record voice** : Record your voice menu , Default is *9 .
- Play voice** : Play your record voice menu ,Default is *10 .
- Default voice** : To set default voice menu, Default is *11 .
- Password** : This is record / default voice password , Default is 1234

Answer Extension enable you to record the customized voice menu remotely from a registered IP-Phone.

- Answer extension** : Call from registered IP-Phone to record the voice menu.

Call Parking

Build a calling rule for IP Phone to park the calls during the phone conversation.

IP PBX Setup

• Call Parking

Extension to Dial for Parking Calls	<input type="text" value="700"/>	
What extension to park calls on	<input type="text" value="701-720"/>	Ex:100-150
Number of seconds a call can be parked for	<input type="text" value="30"/>	
<div><input type="button" value="Submit"/> <input type="button" value="Reset"/></div>		

Extension to Dial for Parking Calls: Set an extension number to dial when need to park the call. Default number is 700.

What extension to park calls on: Set the Extension range for call parking retrieving. (Example: '701-720').

Number of seconds a call can be parked for: Set allowed parking time for the parking call. Default is 30/sec.

Pickup Extension: Set up a number for IP Phone to retrieve back the call. Default is *8.

Timeout for answer on attended transfer: Set a timeout value for answer the transferred call. Default is 30 Sec.

How to use call parking?

1. Make a call the first party.
2. Press extension “# + 700” key to park the call.
3. The Voice guide will tell the user a specific number (701-720) to set parking call (At this moment, the remote extension will hear the reserve sound.)
4. Other remote extension press “retrieve number” to pick up call.

Attendant Extension

Attendant Extension in iPBX system help you to configure internal dial plan for extension setup. It can allow more calls to be handled by IVR from Gateway's FXO, and FXS port.

Attendant Extension Provide 10 sets of IVR.

IP PBX Setup

• Attendant Extension

Attendant Extension Number 1	<input type="text" value="101"/>
Attendant Extension Number 2	<input type="text" value="102"/>
Attendant Extension Number 3	<input type="text" value="103"/>
Attendant Extension Number 4	<input type="text" value="104"/>
Attendant Extension Number 5	<input type="text" value="105"/>
Attendant Extension Number 6	<input type="text" value="106"/>
Attendant Extension Number 7	<input type="text" value="107"/>
Attendant Extension Number 8	<input type="text" value="108"/>
Attendant Extension Number 9	<input type="text" value="109"/>
Attendant Extension Number 10	<input type="text" value="110"/>

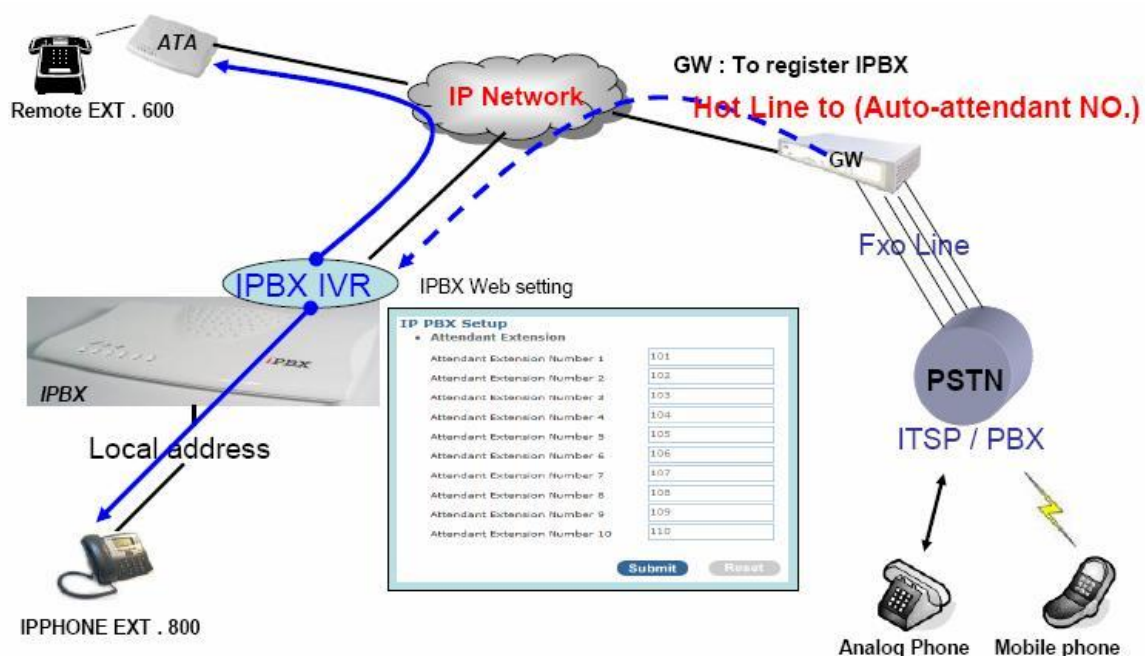
Submit

Reset

The iPBX will handle incoming *Caller ID* and show to remote / local registered IP-Phone.

Note: If your Gateway can bypass Mobile/Analog Phone number, The iPBX will handle incoming caller ID and show to remote / local registered IP-Phone.

Example1:



Dialing Rules

The “**Dialing Rules**” need to be setup when the user uses the method of Peer-to-Peer SIP VoIP call or SIP Proxy Server Mode.

Outgoing Prefix

Outgoing Prefix No	<input type="text" value="9"/>	Ex:9	<button>Change</button>
--------------------	--------------------------------	------	-------------------------

Outgoing Prefix No: Set a prefix number for when making outgoing call via server. This number is used set to initiate the call with the server provider.

Dialing Rules

In the “Dialing Rules” settings: Maximum Entries: **100 records**

Max Rule is 100

Phone NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<button>Insert</button> <button>Change</button>

Phone NO: Phone Number. is the leading digits of the call out dialing number.

Phone NO Pattern: “**N**” single digit from 2 to 9 .

“**Z**” single digit from 1 to 9.

“**X**” single digit from 0 to 9.

“**.**” unlimited length of digit.

Delete Length: Delete Length is the number of digits that will be stripped from beginning of the dialed number.

Prefix NO: Prefix NO is the digits that will be added to the beginning of the dialed number.

Dest. IP/DNS: Destination IP Address / Domain Name is the IP address / Domain Name of the destination ATA (Gateway) that owns this phone number.

Port: Port is port of the destination Gateway / ATA use. (Default is 5060)

General setting

IP-Phone or sip device extension connected iPBX , Extension have call forward / transfer and pickup / voice key ...

• Call Forward Key

Call Forward Alway	Enable	<input type="text" value="*1"/>	(default:*1)
	Disable	<input type="text" value="*2"/>	(default:*2)
Call Forward Busy	Enable	<input type="text" value="*3"/>	(default:*3)
	Disable	<input type="text" value="*4"/>	(default:*4)
Call Forward No Answer	Enable	<input type="text" value="*5"/>	(default:*5)
	Disable	<input type="text" value="*6"/>	(default:*6)

Call forward key

- Call forward always** **Enable:** Dial the “ * 1 + number ” enable call forward always function
 Disable: Dial the “ * 2 ” disable call forward always function
- Call forward Busy** **Enable:** Dial the “ * 3 + number ” enable call forward busy function
 Disable: Dial the “ * 4 ” disable call forward busy function
- Call forward no answer** **Enable:** Dial the “ * 5 + number ” enable call forward no answer function
 Disable: Dial the “ * 6 ” disable call forward no answer function

• Transfer Feature

Attendant Transfer	<input type="text" value="#1"/>	(default:#1)
Blind Transfer	<input type="text" value="#2"/>	(default:#)
Transfer Digit Timeout	<input type="text" value="30"/>	(default:30)

Transfer Feature

- Attendant Transfer:** When you attendant transfer fail, you can definition other transfer number
- Blind Transfer:** Blind Transfer , When Ex: Ext 100 call Ext 200, Ext 200 blind transfer to Ext 300 , Ignore the Ext.300 status, the Ext.200 will immediately on-hook
- Transfer Digit time out:** Set (Attendant/blind) transfer digit time out sec

• Pickup Key

Pickup Extension	<input type="text" value="*8"/>	(default:*8)
------------------	---------------------------------	--------------

Pickup Key

Pickup Extension: Set call pickup (Default is *8)

• Voice Mail

Max Time of A Voice Mail	<input type="text" value="20"/> Seconds(5~20)
Max Number of Messages Per Folder	<input type="text" value="3"/> Seconds
Dial Voice Mail Number	<input type="text" value="*12"/> (default:*12)
Dial My Voice Mail Number	<input type="text" value="*13"/> (default:*13)

Voice Mail

Max time of a voice mail: Set a voice mail max time

Max number of messages per folder: Max number of voice mail per folder

Dial voice mail number: Dial “ *12 “ into voice mail guide

Dial my voice mail number: Dial “ *13 + Ext number “ into voice mail guide

• SMTP Setting

SMTP Server IP / Address	<input type="text"/>
SMTP Autheticated User Name	<input type="text"/>
SMTP Autheticated Password	<input type="text"/>

SMTP Setting

SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified.

Input the valid account number , the extension setting voice mail will be been in used

SMTP server IP / Address: Input server IP / Address

SMTP Authentication user name: Input SMTP Authentication user name

SMTP Authentication password: Input SMTP Authentication password

Management

Admin Account

The administrator account can access the management interface through the web browser.

Management

- Administrator Account**

Administrator Name	<input type="text" value="admin"/>
Administrator Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
- Remote Administration**

Remote administration	<input checked="" type="checkbox"/> Enable
Http port for remote	<input type="text" value="8888"/>
Remote administration only from IP	<input type="text" value="0.0.0.0"/>

Submit

Note:

- The administrator name and password are case-sensitive and the “blank” character is an *illegal character*
- Only the administrator account has the ability to change account password.

Administrator Name: Assign a name to represent the administrator account. Maximum 16 characters. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign “_”.

Administrator Password: Assign an administrator password. Maximum 16 characters and minimum 6 characters with mix of digits and letters characters. Legal characters can be the upper letter “A” to “Z”, lower letter “a” to “z”, digit number “0” to “9” and an underscore sign “_”.

Confirm Password: Enter the administrator password again. Remote Administrator allows the device to be configured through the WAN port from the Internet using a web browser. A username and password is still required to access the browser-based management interface.

Remote Administration: Enable/Disable to access from remote site. Default setting is “Disable”.

Http port for remote: If you allowed the access from the remote site, assign the http port used to access the IP-PBX. Default port number is “8888”.

Remote administration only from IP: Internet IP address of the computer that has access to the IP-PBX. Assign the legal IP address.

Example: http://x.x.x.x:8080 where as x.x.x.x is the WAN IP address and 8080 is the port used for the Web-Management interface.

Date & Time

Set up the time manually.

Manual Time setting

Management

• Date/Time

Date Time Set By	<input checked="" type="radio"/> Manual Time Setting <input type="radio"/> NTP Time Server
Time Zone	(GMT+08:00) Beijing, Singapore, Taipei ▼
Daylight Saving	<input type="checkbox"/>
Date Value Setting	Year: 2007 ▼ Month: 08 ▼ Day: 16 ▼
Time Value Setting	Hour: 17 ▼ Minute: 27 ▼ Second: 27 ▼
<input type="button" value="Submit"/>	

Manual Time Setting: Set up the time manually.

NTP Time server

Management

• Date/Time

Date Time Set By	<input type="radio"/> Manual Time Setting <input checked="" type="radio"/> NTP Time Server
Time Zone	(GMT+08:00) Beijing, Singapore, Taipei ▼
Daylight Saving	<input type="checkbox"/>
NTP Update Interval	24 hours (1..1000, default:24)
NTP Server 1	pool.ntp.org
NTP Server 2	
<input type="button" value="Submit"/>	

NTP Time Server: Protocol used to help match your system clock with an accurate time source. For example atomic clock or a server.

Time Zone: Choose your time zone, Default is (GMT+8:00)Beijing,Singapore,Taipei.

Daylight Saving: Enable / Disable ,Default is Disable,time during which clocks are set one hour ahead of local standard time; widely adopted during summer to provide extra daylight in the evenings

NTP Update Interval: Default is 24 hours , This is used to select the frequency of. NTP updates

NTP Server 1: Default is "pool.ntp.org",NTP Server address.

NTP Server 2: Default is empty.

Ping Test

This useful diagnostic utility can be used to check if a computer is on the Internet. It sends ping packets and listens for replies from the specific host. Enter in a host name or the IP address that you want to ping (Packet Internet Groper) and click Ping. *Example: www.yahoo.com or 216.115.108.245*

Management

- PING Test

PING Destination

Ping Destination: Assign a legal IP address.

Save & Restore

All settings can be saving to a local file. Pervious device configuration can also be restored by upload a local file back to the device.

Management

- Save/Restore Setting

Save Save device current configuration to local file
Restore Upload a local file to restore as device configuration:

Factory Default

This function is used to restore all the parameters back to factory default setting. You can use the Save/Restore Setting to check the factory default configuration, after you click on the Set button.

Management

- Factory Default Setting

Set device configuration to Factory default setting:

Firmware Update

You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of your computer. Click on Browse to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade.

Firmware Update

Firmware File	<input type="text"/>	<input type="button" value="瀏覽..."/>	<input type="button" value="Upload"/>
---------------	----------------------	--------------------------------------	---------------------------------------

Firmware Name: select that you want to upgrade Firmware version.

IPBX Scenario Application Sample

